HIPAA vs. ISB -- A Partial Comparison

Web Security Standards	HIPAA Requirement(s)
II.B.2 - Agency must have a documented plan for the use and infrastructure associated with the use of web browsers and e-mail clients which adheres to the following:	
All software used to access the Internet must be approved by an authorized agency authority and must incorporate all provided security patches that are appropriate to the environment in which it is operating	
Only agency approved versions of browser software may be used or downloaded	
All outbound browser traffic will use appropriate technology to prevent disclosure of IP addresses	For open networks such as the internet: implement integrity controls, message authentication and either access controls or encryption. In addition if using the internet for communication of health information, implement: alarms, audit trails, entity authentication and event reporting
Ensure that files are checked for viruses by either: using anti-virus software on the workstation; routing files to a repository server, checking for viruses, and forwarding the files to the appropriate workstation; or control of portable logic or interactive Internet technology (i.e., Java applets, ActiveX)	Security configuration management practices to include virus checking
II.C - All agency web servers must adhere to the following standards for operation and maintenance:	
II.C.1 - Before information is placed on the Internet, it must be reviewed and approved for release in the same manner as other official memos, reports, or other official non-electronic information. Agency must conform to Executive Order 00-03, Public Records Privacy Protections for its Web site information	
II.C.2 - Users are forbidden to download, install or run Web server software without prior approval by an agency authorized system administrator	
II.C.3 - Remote control of Web servers shall be done from the console or properly secured sessions using high confidence level authentication	
II.C.4 - Web server software and software of the underlying operating system shall employ all security patches and configuration options appropriate to the environment in which it is operating	
II.C.5 - A public Web server shall not serve as a repository for confidential data	